# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-076135
(43)Date of publication of application : 14.03.2000

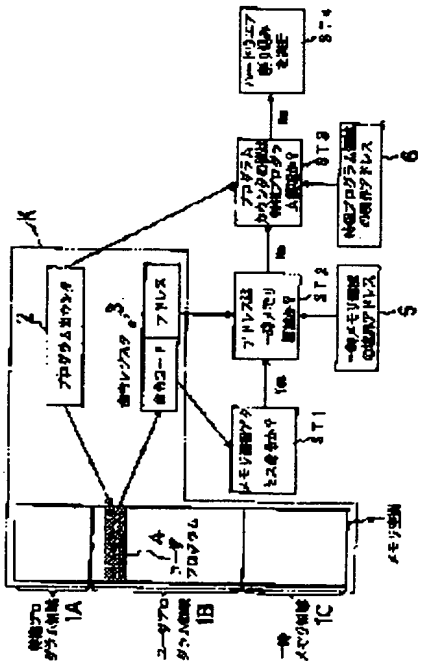
(51)Int.Cl. G06F 12/14
G06K 17/00
G06K 19/073
G06K 19/07

(21)Application number : 10-242304
(22)Date of filing : 27.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HOSODA YASUHIRO
SUZUKI KATSUHIKO

## (54) MEMORY PROTECTIVE METHOD FOR PROCESSOR AND IC CARD FOR PROTECTING MEMORY OF PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the memory protective method of a processor and an IC card for protecting the memory of the processor capable of inhibiting unauthorized access to the memory and securing security even when a program is added to the memory.
SOLUTION: Together with the memory for dividing a memory space 1 into a privilege program area 1A for storing a variety of common service programs, a user program area 1B for storing a user program 4 downloaded by terminal equipment and a temporary memory area 1G to be temporarily used at the execution of the respective programs stored in the user program area 1B and the privilege program area 1A, a control means for performing access from the user program 4 to somewhere other than the temporary memory area 1C through a monitor and stopping the execution of the user program 4 for the unauthorized access to somewhere other than the temporary memory area 1C is provided.



LEGAL STATUS

[Date of request for examination] 18.04.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－76135
（P2000－76135A）
(43)公開日　平成12年３月14日(2000.3.14)

| (51)Int.Cl.' | | 識別記号 | FI | | テーマコード'（参考） |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３２０ | Ｇ０６Ｆ 12/14 | ３２０Ａ | ５Ｂ０１７ |
| Ｇ０６Ｋ | 17/00 | | Ｇ０６Ｋ 17/00 | Ｅ | ５Ｂ０３５ |
| | 19/073 | | 19/00 | Ｐ | ５Ｂ０５８ |
| | 19/07 | | | Ｎ | |

審査請求　未請求　請求項の数24　ＯＬ　（全９頁）

(21)出願番号　特願平10－242304

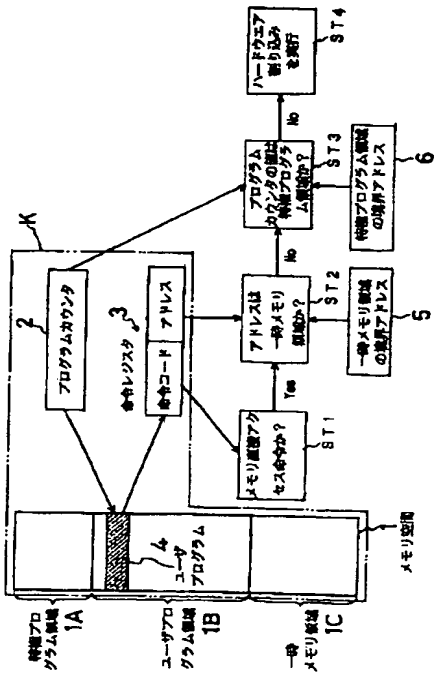
(22)出願日　平成10年８月27日(1998.8.27)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　細田　泰弘
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　鈴木　勝彦
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

最終頁に続く

(54)【発明の名称】　プロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカード

(57)【要約】
【課題】メモリへの不正アクセスを禁止し、メモリにプログラムが追加されてもセキュリティ確保を可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカードの提供。
【解決手段】メモリ空間１を、種々の共通サービスプログラムを格納する特権プログラム領域１Ａと、端末装置によりダウンロードされたユーザプログラム４を格納するユーザプログラム領域１Ｂと、ユーザプログラム領域１Ｂ及び特権プログラム領域１Ａに格納された各プログラムの実行時に一時的に使用する一時メモリ領域１Ｃとに区分するメモリと共に、ユーザプログラム４から一時メモリ領域１Ｃ以外へのアクセスはモニタを経由して行い一時メモリ領域１Ｃ以外への不正なアクセスはユーザプログラム４の実行を止める制御手段を具備するという特徴。



1

【特許請求の範囲】
【請求項１】ＣＰＵとメモリとを有するプロセッサに小規模のハードウエアの追加とロジックにより、当該プロセッサのメモリ領域にユーザプログラムを追加・変更しても、当該メモリ領域への不正なアクセスを不可能にする、
ことを特徴とするプロセッサのメモリ保護方法。
【請求項２】小規模のハードウエアは、
ウインドウ回路を含む、
ことを特徴とする請求項１に記載のプロセッサのメモリ保護方法。
【請求項３】追加・変更は、
前記プロセッサ対応の端末装置により行われる、
ことを特徴とする請求項１又は２に記載のプロセッサのメモリ保護方法。
【請求項４】プロセッサは、
ＩＣカード用である、
ことを特徴とする請求項１、２又は３に記載のプロセッサのメモリ保護方法。
【請求項５】プロセッサは、
ＣＰＵとメモリを有する１チップマイクロコンピュータ用である、
ことを特徴とする請求項１、２又は３に記載のプロセッサのメモリ保護方法。
【請求項６】メモリは、
各種共通のサービスプログラムを格納する特権プログラム領域と、
前記変更・追加されたユーザプログラムを含むユーザプログラムを格納するユーザプログラム領域と、
前記特権プログラム領域、前記ユーザプログラム領域に格納されたプログラムが実行される際に一時的に使用される一時メモリ領域との三領域に区分される、
ことを特徴とする請求項１、２、３、４又は５に記載のプロセッサのメモリ保護方法。
【請求項７】一時メモリ領域は、
前記メモリに格納された如何なるプログラムを実行するに当たり何の制約も受けない、
ことを特徴とする請求項６に記載のプロセッサのメモリ保護方法。
【請求項８】ロジックは、
プログラムカウンタの値が前記ユーザプログラム領域を指している場合には、
前記一時メモリ領域へのアクセスのみを許可すると共に他の領域へのアクセスでは例外処理を行う様に制御される、
ことを特徴とする請求項６又は７に記載のプロセッサのメモリ保護方法。
【請求項９】例外処理は、
ハードウエアの割り込みを生じさせることにより開始される、

2

ことを特徴とする請求項８に記載のプロセッサのメモリ保護方法。
【請求項１０】ロジックは、
前記ユーザプログラム領域に格納されたユーザプログラムから前記一時メモリ領域以外へアクセスの必要性がある場合には、
前記アクセスの正当性の確認を行う、
ことを特徴とする請求項６、７、８又は９に記載のプロセッサのメモリ保護方法。
【請求項１１】アクセスの正当性の確認は、
前記特権プログラム領域に格納されたサービスプログラムを呼出した後に、
前記サービスプログラムにより前記アクセスの正当性の判断を行う、
ことを特徴とする請求項１０に記載のプロセッサのメモリ保護方法。
【請求項１２】判断は、
前記呼出しの前に前記ユーザプログラムが必要とする、前記ユーザプログラム領域のデータに対応した保護キーに相当する情報と当該データのアドレスを前記一時メモリ領域に書き込み、
前記呼出しの後、
前記サービスプログラムにより、前記一時メモリ領域に書き込まれた前記保護キーに相当する情報と、前記ユーザプログラム領域に格納された前記データの保護キーとを照合した結果、一致すれば、アクセスの許可をする、
ことを特徴とする請求項１１に記載のプロセッサのメモリ保護方法。
【請求項１３】アクセスの許可は、
前記データを前記一時メモリ領域に複写した後に、
制御を前記ユーザプログラムに戻す、
ことを特徴とする請求項１２に記載のプロセッサのメモリ保護方法。
【請求項１４】メモリ領域を、
種々の共通サービスプログラムを格納する特権プログラム領域と、
端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、
当該ユーザプログラム領域及び前記特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、
前記ユーザプログラムから前記一時メモリ領域以外へのアクセスはモニタを経由して行い、当該一時メモリ領域以外への不正なアクセスに対して当該ユーザプログラムの実行を止める制御手段を具備する、
ことを特徴とするプロセッサのメモリを保護されたＩＣカード。
【請求項１５】制御手段は、
プログラムカウンタの値が前記ユーザプログラム領域を指している際は前記一時メモリ領域以外の直接アクセス

を禁止し、当該一時メモリ領域以外のへのアクセスが必要な際は当該特権プログラム領域に存在するサービスプログラムを経由し、当該特権プログラム領域を指している際は全てのメモリ領域へのアクセスを可能とする制御手段である、
ことを特徴とする請求項１４に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項１６】制御手段は、
前記プログラムカウンタの値を読み出した後に指定された番地の命令を読み出す命令フェッチ回路と、
当該命令フェッチ回路から前記指定された番地の命令を格納する命令レジスタと、
当該命令レジスタの値をデコードする命令デコード回路と、
当該命令デコード回路に接続されたアドレス演算回路と、
前記命令デコード回路に接続されたラッチと、
前記プログラムカウンタに接続され前記特権プログラム領域の境界アドレスとの関係を判断するウインドウ回路と、
前記アドレス演算回路の出力結果及び演算終了通知を受け、一時メモリ領域の境界アドレスとの関係を判断する別のウインドウ回路と、
前記ラッチと前記ウインドウ回路と前記別のウインドウ回路との各出力を判断する論理回路と、
当該論理回路からの出力により、前記プログラムカウンタに予め特権プログラム領域に設けてある割り込みベクトルによりアドレスをロードする割り込み回路と、を具備する、
ことを特徴とする請求項１４又は１５に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項１７】命令デコード回路は、
当該命令デコード回路の前記命令レジスタの値に対する結果の実行が直接前記メモリ領域にアクセスを必要とする場合には、前記ラッチに対する出力をアサートすると共に前記アドレス演算回路を作動させる、
ことを特徴とする請求項１６に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項１８】制御手段は、
前記メモリと共に一体構成される、
ことを特徴とする請求項１４、１５、１６又は１７に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項１９】共通サービスプログラムは、
前記ＩＣカード上のファイルを管理するプログラムを含む、
ことを特徴とする請求項１４、１５、１６、１７又は１８に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項２０】ＩＣカード上のファイルを管理するプログラムは、
データアクセス用サービスプログラムである、
ことを特徴とする請求項１９に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項２１】前記データアクセス用サービスプログラムは、
前記ユーザプログラム領域に格納されたユーザプログラムが前記一時メモリ領域以外にアクセス要求すると呼び出され、
前記ユーザプログラムが前記一時メモリ領域に書き込みした前記アクセス要求の正当性を示す保護キーに相当する情報及び前記アクセス要求先のアドレスを元にして、書き込まれた当該保護キーに相当する情報と前記ユーザプログラム領域に格納されたアクセス要求先のアドレスの情報に対応した保護キーとを照合した後、
一致すれば前記アクセスを許可し実行する一連の処理プログラムである、
ことを特徴とする請求項２０に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項２２】一連の処理プログラムは、
前記アクセス要求先のアドレスの情報を、前記一時メモリ領域に複写し、
ユーザプログラムに戻る前記実行機能を含む、
ことを特徴とする請求項２１に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項２３】前記ウインドウ回路は、
前記特権プログラム領域の境界アドレスを固定値化する特権プログラム領域の境界アドレス固定値回路に接続する、
ことを特徴とする請求項１７、１８、１９、２０又は２１に記載のプロセッサのメモリを保護されたＩＣカード。
【請求項２４】前記別のウインドウ回路は、
前記一時メモリ領域の境界アドレスを固定値化する一時メモリ領域の境界アドレス固定値回路に接続する、
ことを特徴とする請求項１７、１８、１９、２０、２１又は２２に記載のプロセッサのメモリを保護されたＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード等のセキュリティを必要とする分野に使用される１チップマイクロコンピュータ上のユーザプログラムからの不正メモリアクセスに対して保護する、プロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカードである。
【０００２】
【従来の技術】従来、ＩＣカード用の１チップマイクロコンピュータ（チップ）は、マスクロム上にプログラムを、ＥＥＰＲＯＭ等の不揮発性メモリにユーザデータを格納し、外部端末装置より発行されるコマンドをマスク

ロム上に書き込まれたプログラムが解釈し実行するものが一般的であった。そして、マスクロム上に書き込まれたプログラムは外部からソフト的な手段により破壊することは不可能であるため、予めマスクロム作成者により十分なセキュリティ上の確認を経て作成されたプログラムはユーザデータに対する権限外の不当なアクセスは起きないと考えられている。

【０００３】しかしながら、最近のＩＣカードアプリケーションの拡大に伴い、一度発行したＩＣカード上にプログラムの追加・変更を、ＩＣカードアプリケーション発行機関から要求されているのが現状である。これは、ユーザにとっても複数のカードを持ち歩く必要性がなく、一枚のＩＣカードで複数のサービスを享受できる点で利点が大きい。

【０００４】この要求を実現するために、ユーザデータだけでなくアプリケーションプログラムも不揮発性メモリに記憶させ、チップ作成後にダウンロードにより変更・追加が可能とするＩＣカードが登場している。

【０００５】

【発明が解決しようとする課題】上記のようなＩＣカードでは、チップ作成時において既にＩＣアプリケーションが他のアプリケーションが有するデータへの不正なアクセスを不可能とすることを確認するのは無理であるので、別途新たにメモリ保護機能を当該チップ内に持たす必要性がある。

【０００６】このメモリ保護の実現方法として、先ずこれまでのプロセッサの歴史で確立されてきた種々のハード的な仕掛けをプロセッサ上に盛り込むことが考えられ、限界レジスタ方式、キー方式、アクセスコントロール方式、リングプロテクション方式（中澤喜三朗著「計算機アーキテクチャ構成方式」ｐｐ．１４０－１４３、朝倉書店１９９５年）などが考えられる。

【０００７】しかしながら、これらの方式は元々マルチプログラミングを前提としており、現状のチップはシングルタスクであり、またＩＣカード用チップは低コストが要求されるため、設計が複雑になること、ハード量の不必要な増加を招くこと、命令の実行時間が長くなることなどの面において問題をはらんでいる。

【０００８】一方、ソフトのみでメモリ保護を実現することも選択肢としてありうる。これはいわゆる仮想計算機のチップ上に実装し、そこにメモリ保護機能を持たす方式である。Ｊａｖａ　Ｃａｒｄ（ｈｔｔｐ：／／ｊａｖａ．ｓｕｎ．ｃｏｍ）、Ｍｕｌｔｏｓ（ｈｔｔｐ：／／ｗｗｗ．ｍｕｌｏｓ．ｃｏｍ）等はこの方式によっている。

【０００９】しかしながら、この方式が意味を持つためには、チップ上へのＣＰＵネイティブコードのダウンロードを禁止し、仮想計算機のコードのみを可とする必要がある。仮想計算機上では、メモリアクセスの正当性をソフトウエアにより確認するため性能上のオーバーヘッドがあり、１０倍乃至数十倍程度の実行性能が低下することを回避することができない。



【００１０】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。

【００１１】本発明の第１の目的は、簡便なハードウエアによりメモリの不正アクセスを禁止し、プロセッサ上にプログラムを追加してもセキュリティ確保を可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカードを提供せんとするものである。

【００１２】本発明の第２の目的は、複数のアプリケーションの性能をオーバーヘッドなく実行可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカードを提供せんとするものである。

【００１３】本発明の第３の目的は、命令の実行に長時間を必要とせずにセキュリティを大幅に向上させるプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたＩＣカードを提供せんとするものである。

【００１４】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００１５】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、ＣＰＵとメモリとを有するプロセッサに小規模のハードウエアの追加とロジックにより、プロセッサのメモリ領域にユーザプログラムを追加変更しても、当該メモリ領域への不正なアクセスを不可能にするという特徴を有する。

【００１６】本発明カードは、上記課題の解決に当たり、メモリ領域を種々の共通サービスプログラムを格納する特権プログラム領域と、端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、当該ユーザプログラム領域及び当該特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、当該ユーザプログラムから当該一時メモリ領域以外へのアクセスはモニタを経由して行い当該一時メモリ領域以外への不正なアクセスは当該ユーザプログラムの実行を止める制御手段を具備するという特徴を有する。

【００１７】更に、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、上記目的を達成するように為される。

【００１８】本発明方法の第１の特徴は、ＣＰＵとメモリとを有するプロセッサに小規模のハードウエアの追加とロジックにより、当該プロセッサのメモリ領域にユーザプログラムを追加変更しても、当該メモリ領域への不正なアクセスを不可能にするプロセッサのメモリ保護方法の構成採用にある。

【００１９】本発明方法の第２の特徴は、上記本発明方法の第１の特徴における小規模のハードウエアが、ウイ

ンドウ回路を含んでなるプロセッサのメモリ保護方法の構成採用にある。

【００２０】本発明方法の第３の特徴は、上記本発明方法の第１又は第２の特徴における追加・変更が、前記プロセッサ対応の端末装置により行われてなるプロセッサのメモリ保護方法の構成採用にある。

【００２１】本発明方法の第４の特徴は、上記本発明方法の第１、第２又は第３の特徴におけるプロセッサが、ＩＣカード用であるプロセッサのメモリ保護方法の構成採用にある。

【００２２】本発明方法の第５の特徴は、上記本発明方法の第１、第２又は第３の特徴におけるプロセッサが、ＣＰＵとメモリを有する１チップマイクロコンピュータ用であるプロセッサのメモリ保護方法の構成採用にある。

【００２３】本発明方法の第６の特徴は、上記本発明方法の第１、第２、第３、第４又は第５の特徴におけるメモリが、各種共通のサービスプログラムを格納する特権プログラム領域と、前記変更・追加されたユーザプログラムを含むユーザプログラムを格納するユーザプログラム領域と、前記特権プログラム領域、前記ユーザプログラム領域に格納されたプログラムが実行される際に一時的に使用される一時メモリ領域との三領域に区分されてなるプロセッサのメモリ保護方法の構成採用にある。

【００２４】本発明方法の第７の特徴は、上記本発明方法の第６の特徴における一時メモリ領域が、前記メモリに格納された如何なるプログラムを実行するに当たり何の制約も受けないプロセッサのメモリ保護方法の構成採用にある。

【００２５】本発明方法の第８の特徴は、上記本発明方法の第６又は第７の特徴におけるロジックが、プログラムカウンタの値が前記ユーザプログラム領域を指している場合には、前記一時メモリ領域へのアクセスのみを許可すると共に他の領域へのアクセスでは例外処理を行う様に制御されてなるプロセッサのメモリ保護方法の構成採用にある。

【００２６】本発明方法の第９の特徴は、上記本発明方法の第８の特徴における例外処理が、ハードウエアの割り込みを生じさせることにより開始されてなるプロセッサのメモリ保護方法の構成採用にある。

【００２７】本発明方法の第１０の特徴は、上記本発明方法の第６、第７、第８又は第９の特徴におけるロジックが、前記ユーザプログラム領域に格納されたユーザプログラムから前記一時メモリ領域以外へアクセスの必要性がある場合には、前記アクセスの正当性の確認を行ってなるプロセッサのメモリ保護方法の構成採用にある。

【００２８】本発明方法の第１１の特徴は、上記本発明方法の第１０の特徴におけるアクセスの正当性の確認が、前記特権プログラム領域に格納されたサービスプログラムを呼出した後に、前記サービスプログラムにより前記アクセスの正当性の判断を行ってなるプロセッサのメモリ保護方法の構成採用にある。

【００２９】本発明方法の第１２の特徴は、上記本発明方法の第１１の特徴における判断が、前記呼出し前に前記ユーザプログラムが必要とする、前記ユーザプログラム領域のデータに対応した保護キーに相当する情報と当該データのアドレスを前記一時メモリ領域に書き込み、前記呼出しの後、前記サービスプログラムにより、前記一時メモリ領域に書き込まれた前記保護キーに相当する情報と、前記ユーザプログラム領域に格納された前記データの保護キーとを照合した結果、一致すれば、アクセスの許可を行なってなるプロセッサのメモリ保護方法の構成採用にある。

【００３０】本発明方法の第１３の特徴は、上記本発明方法の第１２の特徴におけるアクセスの許可が、前記データを前記一時メモリ領域に複写した後に、制御を前記ユーザプログラムに戻してなるプロセッサのメモリ保護方法の構成採用にある。

【００３１】一方、本発明カードの第１の特徴は、メモリ領域を、種々の共通サービスプログラムを格納する特権プログラム領域と、端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、当該ユーザプログラム領域及び前記特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、前記ユーザプログラムから前記一時メモリ領域以外へのアクセスはモニタを経由して行い、当該一時メモリ領域以外への不正なアクセスに対して当該ユーザプログラムの実行を止める制御手段を具備してなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３２】本発明カードの第２の特徴は、上記本発明カードの第１の特徴における制御手段が、プログラムカウンタの値が前記ユーザプログラム領域を指している際は前記一時メモリ領域以外の直接アクセスを禁止し、当該一時メモリ領域以外のへのアクセスが必要な際は当該特権プログラム領域に存在するサービスプログラムを経由し、当該特権プログラム領域を指している際は全てのメモリ領域へのアクセスを可能とする制御手段であるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３３】本発明カードの第３の特徴は、上記本発明カードの第１又は第２の特徴における制御手段が、前記プログラムカウンタの値を読み出した後に指定された番地の命令を読み出す命令フェッチ回路と、当該命令フェッチ回路から前記指定された番地の命令を格納する命令レジスタと、当該命令レジスタの値をデコードする命令デコード回路と、当該命令デコード回路に接続されたアドレス演算回路と、前記命令デコード回路に接続されたラッチと、前記プログラムカウンタに接続され前記特権プログラム領域の境界アドレスとの関係を判断するウイ

ンドウ回路と、前記アドレス演算回路の出力結果及び演算終了通知を受け、一時メモリ領域の境界アドレスとの関係を判断する別のウインドウ回路と、前記ラッチと前記ウインドウ回路と前記別のウインドウ回路との各出力を判断する論理回路と、当該論理回路からの出力により、前記プログラムカウンタに予め特権プログラム領域に設けてある割り込みベクトルによりアドレスをロードする割り込み回路と、を具備してなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３４】本発明カードの第４の特徴は、上記本発明カードの第３の特徴における命令デコード回路が、当該命令デコード回路の前記命令レジスタの値に対する結果の実行が直接前記メモリ領域にアクセスを必要とする場合には、前記ラッチに対する出力をアサートすると共に前記アドレス演算回路を作動させてなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３５】本発明カードの第５の特徴は、上記本発明カードの第１、第２、第３又は第４の特徴における制御手段が、前記メモリと共に一体構成されてなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３６】本発明カードの第６の特徴は、上記本発明カードの第１、第２、第３、第４又は第５の特徴における共通サービスプログラムが、前記ＩＣカード上のファイルを管理するプログラムを含んでなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３７】本発明カードの第７の特徴は、上記本発明カードの第６の特徴におけるＩＣカード上のファイルを管理するプログラムが、データアクセス用サービスプログラムであるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３８】本発明カードの第８の特徴は、上記本発明カードの第７の特徴におけるデータアクセス用サービスプログラムが、前記ユーザプログラム領域に格納されたユーザプログラムが前記一時メモリ領域以外にアクセス要求すると呼び出され、前記ユーザプログラムが前記一時メモリ領域に書き込みした前記アクセス要求の正当性を示す保護キーに相当する情報及び前記アクセス要求先のアドレスを元にして、書き込まれた当該保護キーに相当する情報と前記ユーザプログラム領域に格納されたアクセス要求先のアドレスの情報に対応した保護キーとを照合した後、一致すれば前記アクセスを許可し実行する一連の処理プログラムであるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００３９】本発明カードの第９の特徴は、上記本発明カードの第８の特徴における一連の処理プログラムが、前記アクセス要求先のアドレスの情報を、前記一時メモリ領域に複写し、ユーザプログラムに戻る前記実行機能を含んでなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００４０】本発明カードの第１０の特徴は、上記本発明カードの第４、第５、第６、第７又は第８の特徴における前記ウインドウ回路が、前記特権プログラム領域の境界アドレスを固定値化する特権プログラム領域の境界アドレス固定値回路に接続してなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００４１】本発明カードの第１１の特徴は、上記本発明カードの第４、第５、第６、第７、第８又は第９の特徴における前記別のウインドウ回路が、前記一時メモリ領域の境界アドレスを固定値化する一時メモリ領域の境界アドレス固定値回路に接続してなるプロセッサのメモリを保護されたＩＣカードの構成採用にある。

【００４２】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を示すカード例及び方法例を説明し、更にカード例、方法例を用いた実施例をあげて説明する。

【００４３】（カード例）図１は、本カード例のプロセッサのメモリを保護されたＩＣカードＫに関する基本構成を示したものであり、同時に（下記する）カード例に対応する方法例の流れについても示したものである。なお、同図は説明上重要な部分のみを示しており、プログラムカウンタ２、命令レジスタ３の他通常のプロセッサ（特にマイクロプロセッサ）に具備されるレジスタ、入出力関連、クロック等は図示していないが、一般の論理回路、ディジタル回路、情報回路等にして周知であるので省略する。

【００４４】本カード例の対象は、１チップ上に通常の計算機でいう外部記憶、内部記憶が集積されるため、特に区別することなく、一つのメモリ空間１上の領域として考えることが可能である。そこで、この一つのメモリ空間１を三区分し、メモリ空間１を特権プログラム領域１Ａ、ユーザプログラム領域１Ｂ、一時メモリ領域１Ｃとする。

【００４５】特権プログラム領域１Ａは、ＩＣカードＫ上のファイル管理をはじめとする各種の共通のサービスプログラムを格納される領域である。ユーザプログラム領域１Ｂは、（図示しない）端末装置からダウンロードされたユーザプログラム４が格納される領域である。一時メモリ領域１Ｃは、特権プログラム領域１Ａに格納された特権プログラム、ユーザプログラム４が実行時に一時的に使用する領域である。

【００４６】ここで、特権プログラムからは全てのメモリ空間１への読み書き可能である。しかし、ユーザプログラム４からは一時メモリ領域１Ｃのみがアクセス可能であり、それ以外の領域への不正なアクセスを試みるとハードウエア割込みを生ぜしめユーザプログラム４の実行を中断する。

【００４７】（方法例）本方法例は、上記カード例に適用させたものであり、図１を参照しながら説明する。

【００４８】ＩＣカードＫのメモリ空間１上に格納され

るプログラムはプログラムカウンタ２の値に従って読み出され、逐次デコード、実行される。この命令デコードの際、メモリの内容をアクセスする要求が命令中に含まれている否かを判断する（ＳＴ１）。

【００４９】もし含まれている場合には、（１）プログラムカウンタ２の値が、特権プログラム領域１Ａを指していれば、全ての領域へのアクセスを許可し、（２）プログラムカウンタ２の値がユーザプログラム領域１Ｂを指していれば、一時メモリ領域１Ｃへのアクセスのみ許可する。他の領域へのアクセスであれば、ハードウエア割り込みを生じさせ、例外処理を開始する（ＳＴ２、ＳＴ３、ＳＴ４）。ここで、ユーザプログラム４から一時メモリ領域１Ｃ以外へのアクセスが必要であれば、特権プログラム領域１Ａに格納されているサービスプログラムを呼出し、サービスプログラムはアクセス要求が正当なものかを判断した上で許可するか否かを決定する。

【００５０】なお、本方法例は、ＩＣカードＫのみならず、通常のＣＰＵとメモリを有する１チップマイクロコンピュータであっても良い。

【００５１】

【実施例】（実施例１）図２は、上記本実施形態例の実施例を示したものである。同図を参照しながら、説明する。

【００５２】（１）命令フェッチ回路７は、プログラムカウンタ２の値を読み出し、そこで指定されている番地の命令をメモリ８よりメモリ入出力回路９を介して読み出し、命令レジスタ３に格納する。

【００５３】（２）命令レジスタ３の値は、命令デコード回路１０によりデコードされ、その結果に従い命令が実行される。ここで、当該命令が直接メモリ８領域へのアクセスを必要とするものであれば、信号線１１がアサートされると同時にアドレス演算回路１２が動作しアドレス演算を開始する。信号線１１の情報はラッチ１３に取り込まれる。ここで、ラッチ１３は、内部状態を持つ回路で、クロックの立ち上げ又は立ち下げにより入力信号を取り込み、内部状態がそのまま出力信号になる回路である。

【００５４】（３）アドレス演算が終了し演算終了通知１４がアサートされた時点で、ウインドウ回路１５はアドレス演算回路１２からのアドレス出力１６のアドレスと一時メモリ領域１Ｃの境界アドレス固定値回路５’による一時メモリ領域１Ｃの境界アドレス５との関係を判断し、一時メモリ領域１Ｃを外れているときは出力線をアサートする。

【００５５】（４）ウインドウ回路１７は、プログラムカウンタ２の値と特権プログラム領域１Ａの境界アドレス固定値回路６’による特権プログラム領域１Ａの境界アドレス６との関係を判断し、プログラムカウンタ２の値が特権プログラム領域１Ａを外れているときは出力線をアサートする。ここで、ウインドウ回路１５、１７は、プログラムカウンタ２の値ＰＣと境界アドレス（ＡＤ１、ＡＤ２、但しＡＤ１＜ＡＤ２）を比較し、ＩＦ　ＰＣ＜ＡＤ１　ＯＲ　ＰＣ＞ＡＤ２　ＴＨＥＮ１（アドレスは境界領域を外れているので１を出力する）　ＥＬＳＥ　０　という動作をする回路である。

【００５６】（５）２つのウインドウ回路１５、１７からのそれぞれの出力及びラッチ１３からの出力の論理和を論理和回路１８によりとり、全てがアサートされたとき、割り込み要求出力をアサートする。

【００５７】（６）割込み要求がアサートされると、（図示しない）割り込み要求回路はプログラムカウンタ２に予め特権プログラム領域１Ａの設けてある割り込みベクトルによりアドレスをロードし、割り込み処理を開始する。

【００５８】以上の実施例１では、実質的にウインドウ回路１５、１７を付け加え簡単なロジックにより実現することができるが、本発明の目的を達し下記する効果を奏する他の回路構成、ロジックをとっても何等問題はない。

【００５９】（実施例２）図３は、上記実施例１とは別の実施例を示したものである。同図を参照しながら、本実施例を説明する。

【００６０】（１）ユーザプログラム領域１Ｂは、複数のユーザプログラム（ユーザプログラムＡα、ユーザプログラムＢβ、・・）と複数のデータ（データＡγ、データＢδ、・・）を有し、当該データにはそれぞれ保護キー（保護キーＡε、保護キーＢζ、・・）が付けられている。

【００６１】（２）もし、ユーザプログラムＡαがデータＡγを読み出す必要が生じたときは、ユーザプログラムＡαはデータＡγのアドレスと保護キーに相当する情報を一時メモリ領域１Ｃに書き込み（ＳＴ５）、特権プログラム領域１Ａにあるデータアクセス用サービスプログラムηを呼び出す（ＳＴ６）。

【００６２】（３）サービスプログラムηは、一時メモリ領域１Ｃ上に書き込まれた保護キーとデータＡの保護キーεを照合し、一致すればアクセスを許可する。このときデータＡγの情報は一時メモリ領域１Ｃに複写され、制御はユーザプログラムＡαに戻る。

【００６３】これにより、データの持つ保護キーを予め知っているユーザプログラム以外のアクセスは禁止でき、セキュリティを確保することができる。

【００６４】以上、本発明のカード例、方法例を説明し、更に、その実施例について説明したが、本発明は、プロセッサのメモリを保護すると共に、同時に、メモリのアクセス制御方式について示したものであり、本発明の見方により、プロセッサのメモリ保護方法はプロセッサのメモリアクセス方法としても見ることができ、また、プロセッサのメモリが保護されたＩＣカードは、プロセッサのメモリアクセスが制御されたＩＣカードとし

13　　14

て見ることもできる。

【００６５】

【発明の効果】以上説明したように、本発明によれば、小規模なハードウエア（実質的にはウインドウ回路２つ）の追加と簡単なロジックによりチップのセキュリティを大幅に向上させることができるので、ＩＣカード上へのネイティブコードのダウンロードが可能となり、複数のアプリケーションを性能のオーバーヘッドなく実行することができ、多種多様の要請に応えることができる等の優れた効果を奏する。

【図面の簡単な説明】

【図１】本発明の実施の形態の基本構成を示したものである。

【図２】本発明の実施例１を示したものである。

【図３】本発明の実施例２を示したものである。

【符号の説明】

Ｋ…ＩＣカード

１…メモリ空間

１Ａ…特権プログラム領域

１Ｂ…ユーザプログラム領域

ＩＣ…一時メモリ領域

２…プログラムカウンタ

３…命令レジスタ

４…ユーザプログラム

５…一時メモリ領域の境界アドレス

５’…一時メモリ領域の境界アドレス固定値回路

６…特権プログラム領域の境界アドレス

６’…特権プログラム領域の境界アドレス固定値回路

７…命令フェッチ回路

８…メモリ

９…メモリ入出力回路

１０…命令デコード回路

１１…信号線

１２…アドレス演算回路

１３…ラッチ

１４…演算終了通知

１５、１７…ウインドウ回路

１６…アドレス出力

１８…論理和回路

α…ユーザプログラムＡ

β…ユーザプログラムＢ

γ…データＡ

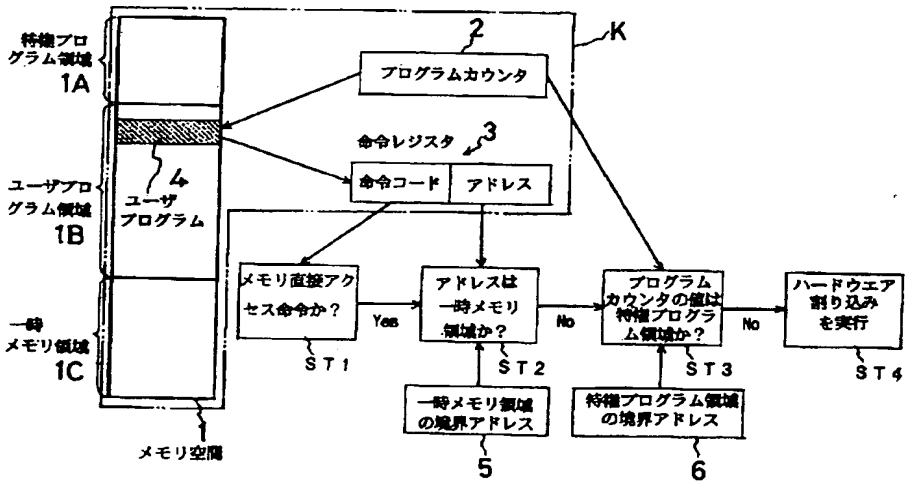
δ…保護キーＡ

ε…データＢ

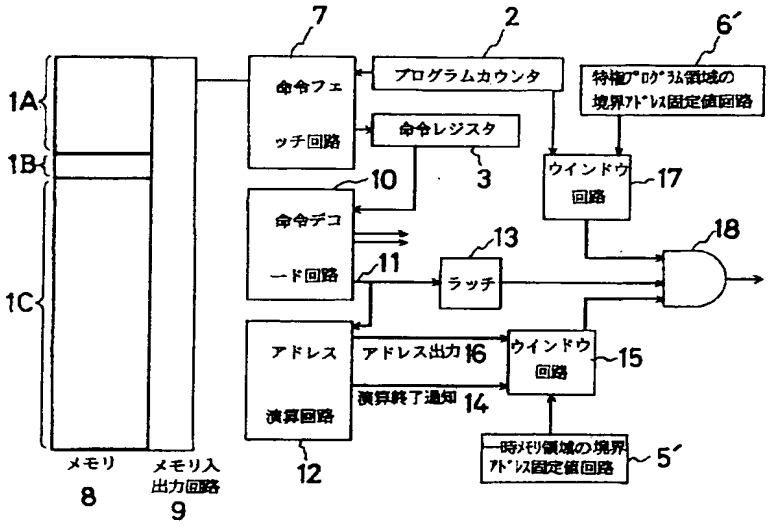
ζ…保護キーＢ

η…データアクセス用サービスプログラム

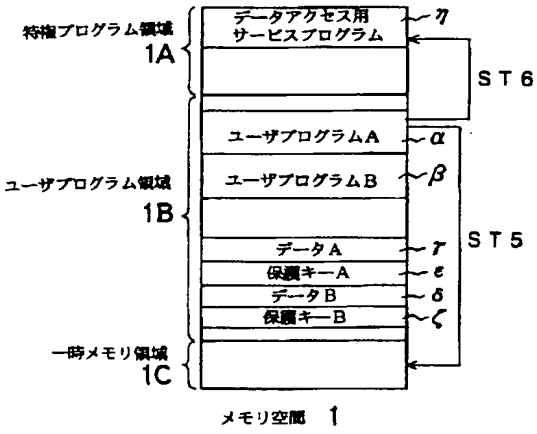
【図１】



【図２】




【図３】




フロントページの続き

Ｆターム(参考)　5B017 AA01 BA01 BA02 BB01 BB03
　　CA13 CA14 CA15
　　5B035 AA13 BB09
　　5B058 CA28 KA31